

ODA3 INSTITUTE

CROSSWALK

GAISSF™-ISO/IEC 42001 Mapping

Artificial Intelligence Management System Alignment Crosswalk

GAISSF-CRO-019 | Informative crosswalk | Draft for Publication

Version 1.0 | Updated 5 October 2026

© 2026 ODA3 Pvt Ltd

Document Control and Reliance Notice

Purpose	Support comparative analysis, ISO-aligned evidence reuse, GAISSF gap identification and residual validation planning.
Mapping direction	GAISSF control → ISO/IEC 42001 clauses, Annex A controls and Annex B guidance.
Normative status	Informative. GAISSF-NOR-001/NOR-004 and ISO/IEC 42001 remain authoritative for their own requirements.
Copyright handling	ISO/IEC text was used as a controlled internal source. This document uses identifiers and original paraphrase and does not reproduce the standard.
Conformity claim	A mapping does not establish equivalence, implementation, certification or compliance.
Validation tooling	Held/internal GAISSF VTS and unpublished test harnesses are not public-package dependencies. Use independently controlled validation appropriate to the control and system context.
Maintenance	Review on GAISSF release, ISO amendment/corrigendum, material validation-method change, or identified mapping defect.
Document ID	GAISSF-CRO-019
Version	1.0
Status	Draft for Publication
GAISSF baseline	59 controls / 9 domains; Applicable-Control Baseline = 52 D1-D8 + applicable D9
External baseline	ISO/IEC 42001:2023, Edition 1 (2023-12)
Updated	5 October 2026

1. Executive Assessment

The complete ISO/IEC 42001:2023 source supplied for the original mapping was used to revalidate all 59 GAISSF controls. ISO/IEC 42001 provides substantial management-system, risk, impact, lifecycle, data, resource, supplier, documentation and assurance coverage. It generally does not prescribe GAISSF's control-specific adversarial, agentic, runtime, content-security or cyber-physical mechanisms. The GAISSF Applicable-Control Baseline is all 52 controls in D1-D8 plus D9 where Physical AI or cyber-physical actuation is in scope.

The principal reuse opportunity is documentary and governance evidence. Evidence reuse remains conditional on scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness. Where the ISO-aligned record does not demonstrate the GAISSF outcome, use an independently controlled validation method appropriate to the control and system context.

2. Mapping Method

- Map by objective, scope, trigger, lifecycle stage, evidence and assurance—not keywords alone.
- Use the most specific ISO location supported by the source, including Annex B where it materially informs interpretation.
- Classify the relationship as Direct enablement, Strong partial, Partial, Supporting or Contextual.
- Record residual requirements and notably absent technical mechanisms in every row.
- Treat evidence reuse as conditional on scope match, authenticity, currency, completeness and operating effectiveness.

3. Relationship Taxonomy

Rating	Meaning	Permitted interpretation
Direct enablement	The GAISSF control explicitly performs or governs the ISO mapping activity.	Supports execution of the mapping process; does not itself establish ISO conformity.
Strong partial	Substantial objective, scope and evidence	Evidence may be reused after qualification;

Rating	Meaning	Permitted interpretation
	overlap.	GAISSF residual remains.
Partial	Related objective or lifecycle coverage with material differences.	Use as supporting evidence only.
Supporting	General governance or assurance support.	Do not treat as control satisfaction.
Contextual	Relevant external-regime or comparison context.	No equivalence or compliance inference.

4. Evidence-Reuse Decision Rules

1. Confirm the ISO AIMS scope matches the GAISSF assessment boundary and AI-system inventory.
2. Verify the record addresses the same control objective, system, period, supplier and lifecycle stage.
3. Reject policy-only evidence where the GAISSF control requires operating-effectiveness or technical test evidence.
4. Preserve provenance, version, approvals, retention, integrity and chain of custody.
5. Execute the selected validation method where the ISO record does not demonstrate the GAISSF pass criteria.
6. Record accepted, partially accepted and rejected evidence with rationale.

5. Notably Absent at the ISO Baseline

ISO/IEC 42001 deliberately permits additional controls beyond Annex A. The following are not prescribed as discrete, testable mechanisms by ISO/IEC 42001 and therefore remain GAISSF residuals where applicable: prompt-injection and jailbreak defenses; least-agency and multi-agent trust controls; model extraction and backdoor testing; LoRA, merge and quantization integrity; AI BOM and model scanning; MCP monitoring and shadow-AI discovery; content filters, leakage tests and watermark robustness; deepfake and AI social-engineering defenses; and functional-safety mechanisms such as safe state, emergency stop, actuator verification and physical-environment integrity monitoring.

6. Detailed 59-Control Crosswalk

Each row must be read together with its residual and validation-boundary fields. ISO locations are reference identifiers; protected ISO text is not reproduced.

GAISSF control	Validation boundary	ISO/IEC 42001 locations	Relationship / confidence	Evidence potentially reusable	Additional GAISSF validation	Residual / notably absent
D1-CTL-01 Dataset Provenance & Poisoning Prevention	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2; 6.1.3; 8.1; 8.2; 8.3; A.4.3; A.6.2.4; A.7.2; A.7.3; A.7.4; A.7.5; B.4.3; B.6.2.4; B.7.2-B.7.5	Strong partial High	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports data, resource, lifecycle, validation, and monitoring governance but does not prescribe this model-integrity technique or GAISSF validation tooling threshold.
D1-CTL-02 Model Extraction Resistance	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2; 6.1.3; 8.1; 8.3; 9.1; A.6.2.4; A.6.2.6; B.6.2.4; B.6.2.6	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports data, resource, lifecycle, validation, and monitoring governance but does not prescribe this model-integrity technique or GAISSF validation tooling threshold.
D1-CTL-03 Behavioral Drift Detection	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2; 6.1.3; 8.1-8.3; 9.1; 10.1-10.2; A.6.2.4; A.6.2.6; A.6.2.8; B.6.2.4; B.6.2.6; B.6.2.8	Strong partial High	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports data, resource, lifecycle, validation, and monitoring governance but does not prescribe this model-integrity technique or GAISSF validation tooling threshold.

GAISSF control	Validation boundary	ISO/IEC 42001 locations	Relationship / confidence	Evidence potentially reusable	Additional GAISSF validation	Residual / notably absent
D1-CTL-04 Federated Learning Poisoning Prevention	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2; 6.1.3; 8.1; A.4.2-A.4.5; A.6.1.3; A.6.2.4; A.7.2-A.7.5; B.4; B.6.1.3; B.6.2.4; B.7	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports data, resource, lifecycle, validation, and monitoring governance but does not prescribe this model-integrity technique or GAISSF validation tooling threshold.
D1-CTL-05 Embedding Space Robustness	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2; 6.1.3; 8.1; 9.1; A.6.2.4; A.6.2.6; B.6.2.4; B.6.2.6	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports data, resource, lifecycle, validation, and monitoring governance but does not prescribe this model-integrity technique or GAISSF validation tooling threshold.
D1-CTL-06 Post-Quantum Model Signing & Crypto Hardening	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.3; 7.5.3; 8.1; A.4.4; A.4.5; A.6.2.3-A.6.2.5; B.4.4-B.4.5; B.6.2.3-B.6.2.5	Supporting Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports data, resource, lifecycle, validation, and monitoring governance but does not prescribe this model-integrity technique or GAISSF validation tooling threshold.

GAISSF control	Validation boundary	ISO/IEC 42001 locations	Relationship / confidence	Evidence potentially reusable	Additional GAISSF validation	Residual / notably absent
D1-CTL-07 LoRA/Adapter Integrity Verification	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2; 6.1.3; 7.5.3; 8.1; A.4.2-A.4.5; A.6.2.3-A.6.2.5; B.4; B.6.2.3-B.6.2.5	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports data, resource, lifecycle, validation, and monitoring governance but does not prescribe this model-integrity technique or GAISSF validation tooling threshold.
D1-CTL-08 Model Merge Attack Detection	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2; 6.1.3; 8.1; A.4.2-A.4.5; A.6.2.3-A.6.2.5; B.4; B.6.2.3-B.6.2.5	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports data, resource, lifecycle, validation, and monitoring governance but does not prescribe this model-integrity technique or GAISSF validation tooling threshold.
D1-CTL-09 Quantization Backdoor Screening	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2; 6.1.3; 8.1; A.6.2.4-A.6.2.6; B.6.2.4-B.6.2.6	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports data, resource, lifecycle, validation, and monitoring governance but does not prescribe this model-integrity technique or GAISSF validation tooling threshold.

GAISSF control	Validation boundary	ISO/IEC 42001 locations	Relationship / confidence	Evidence potentially reusable	Additional GAISSF validation	Residual / notably absent
D2-CTL-01 Direct Prompt Injection Prevention	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.3; 8.1-8.3; 9.1; A.6.1.3; A.6.2.2; A.6.2.4; A.6.2.6; A.9.2; B.6.1.3; B.6.2.2; B.6.2.4; B.6.2.6; B.9.2	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports risk treatment and lifecycle governance but does not expressly prescribe this agentic/runtime attack mechanism, defense design, or GAISSF validation tooling threshold.
D2-CTL-02 Indirect Prompt Injection Prevention	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.3; 8.1-8.3; 9.1; A.6.1.3; A.6.2.2; A.6.2.4; A.6.2.6; A.9.2; A.10.2; B.6; B.9.2; B.10.2	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports risk treatment and lifecycle governance but does not expressly prescribe this agentic/runtime attack mechanism, defense design, or GAISSF validation tooling threshold.
D2-CTL-03 Jailbreak Resistance Testing	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.3; 8.1-8.3; 9.1; A.6.2.4; A.6.2.6; A.9.2; B.6.2.4; B.6.2.6; B.9.2	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports risk treatment and lifecycle governance but does not expressly prescribe this agentic/runtime attack mechanism, defense design, or GAISSF validation tooling threshold.

GAISSF control	Validation boundary	ISO/IEC 42001 locations	Relationship / confidence	Evidence potentially reusable	Additional GAISSF validation	Residual / notably absent
D2-CTL-04 Multi-Modal Injection Defense	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.3; 8.1-8.3; 9.1; A.4.4-A.4.5; A.6.2.4; A.6.2.6; A.9.2; B.4.4-B.4.5; B.6.2.4; B.6.2.6; B.9.2	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports risk treatment and lifecycle governance but does not expressly prescribe this agentic/runtime attack mechanism, defense design, or GAISSF validation tooling threshold.
D2-CTL-05 Function Call/Tool Call Injection Prevention	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.3; 8.1-8.3; A.4.4-A.4.5; A.6.1.3; A.6.2.4; A.6.2.6; A.9.2; B.4.4-B.4.5; B.6; B.9.2	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports risk treatment and lifecycle governance but does not expressly prescribe this agentic/runtime attack mechanism, defense design, or GAISSF validation tooling threshold.
D2-CTL-06 Cross-Context Hijacking Mitigation	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.3; 8.1-8.3; 9.1; A.6.1.3; A.6.2.4; A.6.2.6; A.9.2; B.6; B.9.2	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports risk treatment and lifecycle governance but does not expressly prescribe this agentic/runtime attack mechanism, defense design, or GAISSF validation tooling threshold.

GAISSF control	Validation boundary	ISO/IEC 42001 locations	Relationship / confidence	Evidence potentially reusable	Additional GAISSF validation	Residual / notably absent
D3-CTL-01 Least Agency Enforcement	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	5.3; 6.1.2-6.1.3; 8.1; A.3.2; A.6.1.3; A.6.2.2; A.9.2-A.9.3; B.3.2; B.6; B.9	Strong partial High	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports risk treatment and lifecycle governance but does not expressly prescribe this agentic/runtime attack mechanism, defense design, or GAISSF validation tooling threshold.
D3-CTL-02 Inter-Agent Communication Security	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	5.3; 6.1.2-6.1.3; 8.1; A.3.2; A.4.2; A.6.1.3; A.6.2.4; A.6.2.6; A.10.2-A.10.3; B.3.2; B.4.2; B.6; B.10	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports risk treatment and lifecycle governance but does not expressly prescribe this agentic/runtime attack mechanism, defense design, or GAISSF validation tooling threshold.
D3-CTL-03 Agentic Prompt Chaining Detection	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.3; 8.1-8.3; 9.1; A.6.2.4; A.6.2.6; A.9.2; B.6.2.4; B.6.2.6; B.9.2	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports risk treatment and lifecycle governance but does not expressly prescribe this agentic/runtime attack mechanism, defense design, or GAISSF validation tooling threshold.

GAISSF control	Validation boundary	ISO/IEC 42001 locations	Relationship / confidence	Evidence potentially reusable	Additional GAISSF validation	Residual / notably absent
D3-CTL-04 Embodied AI Safety Controls	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.4; 8.1-8.4; A.4.5; A.5.2-A.5.5; A.6.2.2-A.6.2.6; A.9.2; B.4.5; B.5; B.6; B.9.2	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports risk treatment and lifecycle governance but does not expressly prescribe this agentic/runtime attack mechanism, defense design, or GAISSF validation tooling threshold.
D3-CTL-05 Multi-Agent Trust Chain Attestation	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	5.3; 6.1.3; 7.5.3; 8.1; A.3.2; A.4.2; A.6.2.3-A.6.2.6; A.10.2-A.10.3; B.3.2; B.4.2; B.6; B.10	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports risk treatment and lifecycle governance but does not expressly prescribe this agentic/runtime attack mechanism, defense design, or GAISSF validation tooling threshold.
D3-CTL-06 Persistent Memory Exfiltration Prevention	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.3; 7.5.3; 8.1-8.3; A.6.2.4; A.6.2.6; A.7.2-A.7.5; A.9.2; B.6; B.7; B.9.2	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports risk treatment and lifecycle governance but does not expressly prescribe this agentic/runtime attack mechanism, defense design, or GAISSF validation tooling threshold.

GAISSF control	Validation boundary	ISO/IEC 42001 locations	Relationship / confidence	Evidence potentially reusable	Additional GAISSF validation	Residual / notably absent
D3-CTL-07 Secure Memory Lifecycle Management	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.3; 7.5.3; 8.1; A.6.2.2-A.6.2.8; A.7.2-A.7.6; B.6; B.7	Strong partial High	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports risk treatment and lifecycle governance but does not expressly prescribe this agentic/runtime attack mechanism, defense design, or GAISSF validation tooling threshold.
D4-CTL-01 AI Bill Of Materials (AI Bom) Maintenance	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	4.3; 6.1.2-6.1.3; 7.5; 8.1; A.4.2-A.4.5; A.6.2.3; A.10.2-A.10.3; B.4; B.6.2.3; B.10	Strong partial High	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports resource and supplier governance but does not prescribe the named GAISSF inventory, scanning, monitoring, or discovery mechanism.
D4-CTL-02 Model File & Artifact Scanning	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.3; 8.1; A.4.2-A.4.5; A.6.2.4-A.6.2.5; A.10.2-A.10.3; B.4; B.6.2.4-B.6.2.5; B.10	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports resource and supplier governance but does not prescribe the named GAISSF inventory, scanning, monitoring, or discovery mechanism.

GAISSF control	Validation boundary	ISO/IEC 42001 locations	Relationship / confidence	Evidence potentially reusable	Additional GAISSF validation	Residual / notably absent
D4-CTL-03 Model Hub & Registry Vetting	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.3; 8.1; A.4.2-A.4.5; A.10.2-A.10.3; B.4; B.10	Strong partial High	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports resource and supplier governance but does not prescribe the named GAISSF inventory, scanning, monitoring, or discovery mechanism.
D4-CTL-04 MCP Server Behavioral Monitoring	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.3; 8.1; 9.1; A.4.4-A.4.5; A.6.2.6; A.10.2-A.10.3; B.4.4-B.4.5; B.6.2.6; B.10	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports resource and supplier governance but does not prescribe the named GAISSF inventory, scanning, monitoring, or discovery mechanism.
D4-CTL-05 Third-Party AI Api Security Assessment	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	4.2-4.3; 6.1.2-6.1.3; 8.1; A.10.2-A.10.3; B.10	Strong partial High	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports resource and supplier governance but does not prescribe the named GAISSF inventory, scanning, monitoring, or discovery mechanism.

GAISSF control	Validation boundary	ISO/IEC 42001 locations	Relationship / confidence	Evidence potentially reusable	Additional GAISSF validation	Residual / notably absent
D4-CTL-06 Shadow AI Discovery & Governance	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	4.1-4.3; 6.1.2-6.1.3; 8.1; A.4.2; A.9.2; A.10.2; B.4.2; B.9.2; B.10.2	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports resource and supplier governance but does not prescribe the named GAISSF inventory, scanning, monitoring, or discovery mechanism.
D4-CTL-07 AI Software Composition Analysis (SCA)	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.3; 8.1; A.4.4-A.4.5; A.6.2.3-A.6.2.5; A.10.2-A.10.3; B.4; B.6; B.10	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports resource and supplier governance but does not prescribe the named GAISSF inventory, scanning, monitoring, or discovery mechanism.
D5-CTL-01 Harmful Content Blocking	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.4; 8.1-8.4; 9.1; A.5.2-A.5.5; A.6.2.4; A.6.2.6; A.8.2; A.9.2; B.5; B.6.2.4; B.6.2.6; B.8.2; B.9.2	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports impact, data, lifecycle, and user-information controls but does not prescribe the named technical safeguard or GAISSF validation tooling threshold.

GAISSF control	Validation boundary	ISO/IEC 42001 locations	Relationship / confidence	Evidence potentially reusable	Additional GAISSF validation	Residual / notably absent
D5-CTL-02 PII Leakage Prevention	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.4; 7.5.3; 8.1-8.4; A.5.2-A.5.5; A.6.2.4; A.7.2-A.7.6; A.8.2; B.5; B.6.2.4; B.7; B.8.2	Strong partial High	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports impact, data, lifecycle, and user-information controls but does not prescribe the named technical safeguard or GAISSF validation tooling threshold.
D5-CTL-03 Copyright Detection	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	4.2; 6.1.2-6.1.3; 8.1; A.5.2-A.5.5; A.6.2.4; A.8.2; B.5; B.6.2.4; B.8.2	Supporting Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports impact, data, lifecycle, and user-information controls but does not prescribe the named technical safeguard or GAISSF validation tooling threshold.
D5-CTL-04 AI Watermarking Robustness	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.3; 8.1; 9.1; A.6.2.4; A.6.2.6; A.8.2; B.6.2.4; B.6.2.6; B.8.2	Supporting Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports impact, data, lifecycle, and user-information controls but does not prescribe the named technical safeguard or GAISSF validation tooling threshold.

GAISSF control	Validation boundary	ISO/IEC 42001 locations	Relationship / confidence	Evidence potentially reusable	Additional GAISSF validation	Residual / notably absent
D5-CTL-05 Privacy-By-Design Verification	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	4.2; 6.1.2-6.1.4; 8.1-8.4; A.5.2-A.5.5; A.6.1.3; A.6.2.2-A.6.2.4; A.7.2-A.7.6; B.5-B.7	Strong partial High	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports impact, data, lifecycle, and user-information controls but does not prescribe the named technical safeguard or GAISSF validation tooling threshold.
D5-CTL-06 Privacy-Preserving MI Validation	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.3; 8.1-8.3; 9.1; A.6.2.4; A.7.2-A.7.6; B.6.2.4; B.7	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 supports impact, data, lifecycle, and user-information controls but does not prescribe the named technical safeguard or GAISSF validation tooling threshold.
D6-CTL-01 Human-In-The-Loop For High-Risk Actions	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	5.3; 6.1.2-6.1.4; 8.1; A.3.2; A.5.2-A.5.5; A.6.2.2; A.9.2-A.9.3; B.3.2; B.5; B.6.2.2; B.9	Strong partial High	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 provides strong management-system support, but GAISSF retains its control-specific evidence, test, retention, and operating-effectiveness requirements.

GAISSF control	Validation boundary	ISO/IEC 42001 locations	Relationship / confidence	Evidence potentially reusable	Additional GAISSF validation	Residual / notably absent
D6-CTL-02 Audit Trail Completeness	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	7.5; 8.1; 9.1-9.3; 10.2; A.6.2.8; A.8.5; B.6.2.8; B.8.5	Strong partial High	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 provides strong management-system support, but GAISSF retains its control-specific evidence, test, retention, and operating-effectiveness requirements.
D6-CTL-03 AI Model Card Completeness	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	7.4-7.5; 8.1; A.6.2.3; A.6.2.7; A.8.2; A.8.5; B.6.2.3; B.6.2.7; B.8.2; B.8.5	Strong partial High	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 provides strong management-system support, but GAISSF retains its control-specific evidence, test, retention, and operating-effectiveness requirements.
D6-CTL-04 AI Incident Response Readiness	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	5.3; 7.4-7.5; 8.1; 9.1; 10.2; A.3.3; A.8.3-A.8.5; B.3.3; B.8.3-B.8.5	Strong partial High	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 provides strong management-system support, but GAISSF retains its control-specific evidence, test, retention, and operating-effectiveness requirements.

GAISSF control	Validation boundary	ISO/IEC 42001 locations	Relationship / confidence	Evidence potentially reusable	Additional GAISSF validation	Residual / notably absent
D6-CTL-05 Model Deprecation & Decommissioning	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.3; 7.5.3; 8.1; 10.1-10.2; A.6.2.6-A.6.2.8; B.6.2.6-B.6.2.8	Strong partial High	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 provides strong management-system support, but GAISSF retains its control-specific evidence, test, retention, and operating-effectiveness requirements.
D6-CTL-06 Third-Party AI Vendor Governance	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	4.2-4.3; 6.1.2-6.1.3; 8.1; A.10.2-A.10.3; B.10	Strong partial High	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 provides strong management-system support, but GAISSF retains its control-specific evidence, test, retention, and operating-effectiveness requirements.
D6-CTL-07 AI Resilience & Business Continuity	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.3; 8.1-8.3; 9.1; 10.1-10.2; A.4.2-A.4.6; A.6.2.6; B.4; B.6.2.6	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 provides strong management-system support, but GAISSF retains its control-specific evidence, test, retention, and operating-effectiveness requirements.

GAISSF control	Validation boundary	ISO/IEC 42001 locations	Relationship / confidence	Evidence potentially reusable	Additional GAISSF validation	Residual / notably absent
D7-CTL-H01 AI-Generated Phishing Simulation	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.4; 7.2-7.3; 8.1; A.5.2-A.5.5; A.9.2; B.5; B.9.2	Supporting Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 provides related governance support but does not prescribe the named GAISSF technical or operational mechanism.
D7-CTL-H02 Deepfake Detection Training	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.4; 7.2-7.3; 8.1; A.5.2-A.5.5; A.8.2; A.9.2; B.5; B.8.2; B.9.2	Supporting Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 provides related governance support but does not prescribe the named GAISSF technical or operational mechanism.
D7-CTL-H03 Out-Of-Band Authentication	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.3; 8.1; A.9.2; B.9.2	Supporting Low	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 provides related governance support but does not prescribe the named GAISSF technical or operational mechanism.

GAISSF control	Validation boundary	ISO/IEC 42001 locations	Relationship / confidence	Evidence potentially reusable	Additional GAISSF validation	Residual / notably absent
D7-CTL-H04 AI Social Engineering IR	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.4; 7.2-7.4; 8.1; 10.2; A.3.3; A.5.2-A.5.5; A.8.3-A.8.5; B.3.3; B.5; B.8	Supporting Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 provides related governance support but does not prescribe the named GAISSF technical or operational mechanism.
D7-CTL-H05 AI-Enhanced External Attack Defense	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.3; 8.1-8.3; 9.1; A.6.2.4; A.6.2.6; A.9.2; B.6.2.4; B.6.2.6; B.9.2	Supporting Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 provides related governance support but does not prescribe the named GAISSF technical or operational mechanism.
D8-CTL-01 Eu AI Act Risk Tier Mapping	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	4.1-4.3; 6.1.1-6.1.4; 7.5; 8.1-8.4; A.5; A.8; B.5; B.8	Contextual High	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 does not establish conformity with the external law, regulation, or framework named by this GAISSF control; separate authoritative interpretation and evidence remain required.

GAISSF control	Validation boundary	ISO/IEC 42001 locations	Relationship / confidence	Evidence potentially reusable	Additional GAISSF validation	Residual / notably absent
D8-CTL-02 Iso 42001 Gap Analysis	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	4-10; A.2-A.10; B.2-B.10	Direct enablement High	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 does not establish conformity with the external law, regulation, or framework named by this GAISSF control; separate authoritative interpretation and evidence remain required.
D8-CTL-03 Gpai Technical Documentation Verification	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	4.2; 7.4-7.5; 8.1; A.6.2.3; A.6.2.7; A.8.2; A.8.5; B.6.2.3; B.6.2.7; B.8.2; B.8.5	Contextual High	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 does not establish conformity with the external law, regulation, or framework named by this GAISSF control; separate authoritative interpretation and evidence remain required.
D8-CTL-04 Dora Ict Incident Reporting (Financial Sector)	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	4.2; 7.4-7.5; 8.1; 10.2; A.8.4-A.8.5; A.10.2-A.10.3; B.8.4-B.8.5; B.10	Contextual High	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 does not establish conformity with the external law, regulation, or framework named by this GAISSF control; separate authoritative interpretation and evidence remain required.

GAISSF control	Validation boundary	ISO/IEC 42001 locations	Relationship / confidence	Evidence potentially reusable	Additional GAISSF validation	Residual / notably absent
D8-CTL-05 Nist Sp 800-218A Compliance Check	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.3; 8.1; A.6.1.3; A.6.2.2-A.6.2.5; A.10.2-A.10.3; B.6; B.10	Contextual High	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Qualify ISO/IEC 42001 evidence for matching scope, provenance, authenticity, currency, completeness, relevance and operating effectiveness; independently validate the GAISSF outcome where needed.	ISO/IEC 42001 does not establish conformity with the external law, regulation, or framework named by this GAISSF control; separate authoritative interpretation and evidence remain required.
D9-CTL-01 Physical Harm Boundary Enforcement	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.4; 8.1-8.4; A.4.5; A.5.2-A.5.5; A.6.2.2-A.6.2.5; B.4.5; B.5; B.6.2.2-B.6.2.5	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Where D9 applies, use system- and hazard-appropriate simulation/HIL/physical testing and safe-state/override evidence as applicable; no universal SIL/DAL or certification level is implied.	ISO/IEC 42001 provides risk, impact, resource, and lifecycle governance but does not prescribe this functional-safety or cyber-physical mechanism or its implementation-specific acceptance criteria.
D9-CTL-02 Safe State And Graceful Degradation	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.3; 8.1-8.3; A.6.2.2; A.6.2.4-A.6.2.6; B.6.2.2; B.6.2.4-B.6.2.6	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Where D9 applies, use system- and hazard-appropriate simulation/HIL/physical testing and safe-state/override evidence as applicable; no universal SIL/DAL or certification level is implied.	ISO/IEC 42001 provides risk, impact, resource, and lifecycle governance but does not prescribe this functional-safety or cyber-physical mechanism or its implementation-specific acceptance criteria.

GAISSE control	Validation boundary	ISO/IEC 42001 locations	Relationship / confidence	Evidence potentially reusable	Additional GAISSE validation	Residual / notably absent
D9-CTL-03 Human Override And Emergency Stop	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	5.3; 6.1.2-6.1.4; 8.1; A.3.2; A.5.2-A.5.5; A.6.2.2-A.6.2.5; A.9.2; B.3.2; B.5; B.6; B.9.2	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Where D9 applies, use system- and hazard-appropriate simulation/HIL/physical testing and safe-state/override evidence as applicable; no universal SIL/DAL or certification level is implied.	ISO/IEC 42001 provides risk, impact, resource, and lifecycle governance but does not prescribe this functional-safety or cyber-physical mechanism or its implementation-specific acceptance criteria.
D9-CTL-04 Cyber-Physical Attack Detection	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.3; 8.1-8.3; 9.1; A.4.5; A.6.2.4; A.6.2.6; A.6.2.8; B.4.5; B.6.2.4; B.6.2.6; B.6.2.8	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Where D9 applies, use system- and hazard-appropriate simulation/HIL/physical testing and safe-state/override evidence as applicable; no universal SIL/DAL or certification level is implied.	ISO/IEC 42001 provides risk, impact, resource, and lifecycle governance but does not prescribe this functional-safety or cyber-physical mechanism or its implementation-specific acceptance criteria.
D9-CTL-05 Physical Environment Integrity Monitoring	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.3; 8.1; 9.1; A.4.5; A.6.2.4; A.6.2.6; B.4.5; B.6.2.4; B.6.2.6	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Where D9 applies, use system- and hazard-appropriate simulation/HIL/physical testing and safe-state/override evidence as applicable; no universal SIL/DAL or certification level is implied.	ISO/IEC 42001 provides risk, impact, resource, and lifecycle governance but does not prescribe this functional-safety or cyber-physical mechanism or its implementation-specific acceptance criteria.

GAISSE control	Validation boundary	ISO/IEC 42001 locations	Relationship / confidence	Evidence potentially reusable	Additional GAISSE validation	Residual / notably absent
D9-CTL-06 Actuator Command Verification	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	6.1.2-6.1.3; 8.1-8.3; A.6.2.2; A.6.2.4-A.6.2.6; B.6.2.2; B.6.2.4-B.6.2.6	Partial Medium	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Where D9 applies, use system- and hazard-appropriate simulation/HIL/physical testing and safe-state/override evidence as applicable; no universal SIL/DAL or certification level is implied.	ISO/IEC 42001 provides risk, impact, resource, and lifecycle governance but does not prescribe this functional-safety or cyber-physical mechanism or its implementation-specific acceptance criteria.
D9-CTL-07 Physical Incident Evidence Preservation	Not a public-package dependency; use an independently controlled validation method appropriate to the control and system context.	7.5.3; 8.1; 9.1; 10.2; A.6.2.8; A.8.4-A.8.5; B.6.2.8; B.8.4-B.8.5	Strong partial High	Risk/impact assessments; treatment and SoA records; controlled lifecycle documentation; monitoring, audit, supplier, competence, or communication records applicable to the cited locations.	Where D9 applies, use system- and hazard-appropriate simulation/HIL/physical testing and safe-state/override evidence as applicable; no universal SIL/DAL or certification level is implied.	ISO/IEC 42001 provides risk, impact, resource, and lifecycle governance but does not prescribe this functional-safety or cyber-physical mechanism or its implementation-specific acceptance criteria.

7. Reverse Traceability Summary

ISO location	Primary subject	GAISSF reuse / limitation
Clauses 4-5	Context, scope, leadership, policy, roles	Primarily D6 and D8; supports D3/D4 accountability and boundary decisions.
Clause 6	Risk, impact, treatment, objectives and change planning	Cross-domain support; strongest general bridge to GAISSF control selection and residual controls.
Clause 7	Resources, competence, awareness, communication and documented information	D6/D7 governance evidence and evidence-control support across all domains.
Clause 8	Operational planning, risk treatment and impact assessment	Operational bridge to all domains, but does not define most GAISSF technical mechanisms.
Clauses 9-10	Monitoring, audit, management review, corrective action and improvement	Assurance reuse across all domains; technical retesting remains required.
Annex A.2-A.3	Policy and internal organization	D6 governance; D3/D4 accountability.
Annex A.4	AI resources	D1, D3, D4 and D9 resource/component inventories.
Annex A.5	AI-system impacts	D5, D7, D8 and D9 impact/harm assessment.
Annex A.6	AI lifecycle	Broadest technical-governance overlap across D1-D6 and D9.
Annex A.7	Data for AI systems	D1 and D5 data governance, provenance, quality and preparation.
Annex A.8	Information for interested parties	D5/D6/D8 documentation, concerns, incident communication and reporting.
Annex A.9	Responsible use	D2/D3/D5/D6/D7 use controls and human oversight.
Annex A.10	Third-party and customer relationships	D4 and D6 supplier/shared-responsibility governance.

8. Validation and Certification Boundaries

- Held/internal GAISSF validation tooling is not a dependency of this public crosswalk.
- Demo, mock or placeholder output is not independent assurance evidence.
- GAISSF certification is not currently offered. Any future certification scheme would require separately approved and published governance.
- ISO-aligned evidence may reduce duplicate documentary work but does not waive GAISSF outcome verification, evidence-sufficiency assessment, or independent assurance where required.
- Any validation substitution, inherited evidence or compensating-control decision should be documented with scope, rationale, provenance, limitations and reviewer identity.

9. Source Register

Source	Use
ISO/IEC 42001:2023(E)	Primary external baseline; complete licensed source supplied for original mapping; protected text not redistributed.
GAISSF-NOR-001 v1.0	Authoritative framework, conformance and evidence baseline.
GAISSF-NOR-004 v1.0	Authoritative 59-control catalogue.
GAISSF-NOR-005 v1.0	Controlled terminology.
GAISSF-NOR-006 v1.0	Controlled source and crosswalk citation rules.

10. Publication and Claims Rules

- Publish GAISSE-CRO-019 only as an informative, version-controlled Draft for Publication until independent crosswalk review and explicit publication approval are complete.
- Do not reproduce the supplied ISO/IEC PDF or substantial ISO text.
- Do not state that GAISSE is equivalent to ISO/IEC 42001 or that one certification satisfies the other.
- Identify the exact GAISSE and ISO editions in every mapping claim.
- Publish the DOCX/PDF explanation together with the XLSX register and JSON register.
- Record changes to mappings, relationship ratings, validation-method assumptions or source editions in controlled release notes.

Annex A — Mapping Register Field Definition

Field	Definition
control_id	Stable GAISSE control identifier.
validation_reference / validation_method	Optional validation traceability where the method is published, current and applicable; not a public-package dependency.
iso_42001_references	Clause, Annex A control and Annex B guidance identifiers.
relationship	Nature of overlap without equivalence.
mapping_confidence	Strength of source-based mapping conclusion.
iso_evidence_reuse	Evidence candidates subject to qualification.
additional_gaisse_validation	Residual independent validation or verification action.
gaisse_residual_notably_absent	Specific mechanism or outcome not prescribed by the ISO baseline.